Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 23 July 2003

Current Nationwide Threat Level is

For info click here
www.whitehouse.gov/homeland

Daily Overview

- Government Executive Magazine reports top executives from several large anti−counterfeiting organizations and companies that own intellectual property rights have called for the federal government to bolster efforts to stop terrorists' use of piracy and counterfeiting to fund their activities. (See item 16)
- The Associated Press reports there is a definite risk in using public Internet terminals −− at cybercafes, libraries, airports and other establishments −− which has been demonstrated by recent high−profile cases where software that logs individual keystrokes has been installed on public computers and used to record user names and passwords. (See item 19)
- The Christian Science Monitor reports that U.S. military said Tuesday it had confirmed that Saddam Hussein's two sons, Qusay and Uday, had been killed in a fierce gun battle in the northern city of Mosul. (See item 23)
- The Department of Homeland Security has issued an information bulletin regarding the possible use by terrorists of official identification, uniforms, or vehicles to gain access to sensitive facilities for purposes of planning or carrying out attacks. (See item 24)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 22, Energy Info Source* — **Dominion to study by year−end possible LNG plant expansion. Dominion Resources Inc. of Richmond, VA, will assess the potential of**

expansion opportunities around their new Cove Point, MD, liquefied natural gas (LNG) terminal. The terminal will receive its first commercial shipment within weeks, and **the company wants look at expanding the interstate pipeline grid near the facility**. LNG imports account for 3% of the U.S. natural gas market, but due to increasing demand and constraints on supply, proposals have been made for new terminals, which would increase the market share to 10%. **LNG is natural gas that has been frozen to −270 degrees Fahrenheit, which allows specialized ships and storage tanks to hold 600 times as much gas in the same space, and according to the Energy Information Agency (EIA), it is less likely to catch on fire**. The LNG is converted back to gas before entering the interstate pipeline grid. Also, EIA states that "it takes much longer to convert natural gas to LNG than is does to convert the LNG back into natural gas. It takes about 90 days to fill one of the four storage tanks at Cove Point, while it only takes a day and a half to empty a tank."
Source: http://www.energyinfosource.com/aoi/news−details.cfm?id=1952 3&FLink=

2. *July 22, Reuters* — **PPL restores most power after Pennsylvania thunderstorms. Severe thunderstorms knocked out power to more than 136,000 customers in Pennsylvania on Monday, July 21**. PPL Electric Utilities (PPL) serves those customers, and hopes to have complete power restored by Tuesday, July 22. "**More than 1,000 repair jobs were necessary**," according to Michael Bray, president of PPL, with crews from utilities in Washington, DC, and Virginia assisting in the repair effort.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_07_22_eng−reuters_pma_PPL−RESTORES−MOST−POWER−AFTER−PENN−THUNDERSTORMS&SMContentSet=0

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *July 23, Government Accounting Office* — **Report GAO−03−775: Joint Strike Fighter Acquisition: Managing Competing Pressures Is Critical to Achieving Program Goals. The Joint Strike Fighter (JSF) is a cooperative program between the Department of Defense (DOD) and U.S. allies for developing and producing next generation fighter aircraft to replace aging inventories**. The JSF program is DOD's most expensive aircraft program to date, costing an estimated $200 billion to procure about 2,600 aircraft and related support equipment. To determine the implications of the JSF international program structure, the Government Accounting Office (GAO) identified JSF program relationships and expected benefits and assessed how DOD is managing cost sharing, technology transfer, and partner expectations for industrial return. **GAO is recommending that the Secretary of Defense direct the JSF Program Office to ensure that international supplier planning fully anticipates and mitigates risks associated with technology transfer and that information concerning the selection and management of suppliers is available, closely monitored, and used to**

improve program outcomes.
Source: http://www.gao.gov/highlights/d03775high.pdf

[Return to top]

Banking and Finance Sector

4. *July 22, Washington Post* — **Online identity−theft tactic targeted.** A Los Angeles 17−year−old has settled charges that he used fake Web pages to lure consumers to provide credit card numbers and other personal data, the Federal Trade Commission announced Monday, July 21. The FTC action comes as **reports of identify theft are increasing from 161,886 last year with an expectation of reaching over 200,000 this year**. Industry and consumer groups are warning consumers about a new online scam called "phishing." **Phishing is when a fraudster sends an e−mail to a regular customer of an online service or retailer and tells them that they need to verify their account information**. The customer clicks on a link in the e−mail which takes them to a webpage that looks like that of the online service or retailer. The customer then enters in personal information, such as username, password, credit card numbers, and social security number. The fraudster uses the information to make purchases and access online bank accounts. **Officials are advising consumers to never respond to such e−mails, especially those stating that the company needs the information because of a computer crash, relating that reputable companies will not ask you for that kind of information**.
   Source: http://www.washingtonpost.com/wp−dyn/articles/A25491−2003Jul21.html?referrer=emailarticle

[Return to top]

Transportation Sector

5. *July 22, USA TODAY* — **Fliers flood TSA with inspection gripes.** The federal agency responsible for airport security is overwhelmed with passenger complaints about baggage, seven months after it began inspecting all checked bags for explosives. **The Transportation Security Administration says it's trying to handle complaints better, but as summer travel nears its peak, travelers and some industry officials say improvement can't come fast enough. The TSA says it has received nearly 11,000 claims about damaged bags or lost property since January,** when it began screening all checked baggage. Less than 4% — 385 — have been settled and for an average of $90 a claim. About 350 more are ready to be settled. Anna Heise says the TSA told her it could take as long as a year to settle her $200 claim, which she filed after discovering that a divider was ripped out of her suitcase, which made it useless. The TSA says some passengers are filing complaints with it after being referred by airlines. TSA screeners are supposed to insert a form letter into bags they open, notifying the owner that their bag was opened by security. **The agency is still setting up a baggage claims office, which it hopes to have running by early September, and hiring full−time staff. It now relies mostly on employees borrowed from other departments to process claims.**
   Source: http://www.usatoday.com/travel/news/2003/07/22−tsa.htm

6. *July 22, Sunspot.net* — **Three airlines ease ban on using cell phones: American, Continental, JetBlue allow calls after a plane lands.** At least three airlines, American, Continental and, most recently, JetBlue, have begun allowing passengers to make calls during that seemingly interminable period between when the wheels touch down at the destination and when the passenger actually escapes into the airport building. **Two agencies − the Federal Aviation Administration and Federal Communications Commission − ban cell phone use in aircraft from when the plane's doors are closed for departure to when it lands at the end of the trip, leaving to airline discretion the period after the wheels touch down.** Most carriers simply ban cell phone use altogether. **The FAA, whose ban includes other wireless communications gadgets, is worried about interference with aircraft navigation aids, particularly those on the ground that send radio signals to planes to help pilots stay on course.** Alison Duquette, an FAA spokesperson, says there are no documented incidents of such interference from passenger−carried devices, but "we feel there is a potential for a problem, so we don't allow them." **The FCC bans airborne use of cell phones because a phone broadcasting from 35,000 feet can reach many cell phone towers and play havoc with the system.**
   Source: http://www.sunspot.net/business/bal−bz.airphones22jul22,0,7958713.story?coll=bal−business−headlines

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

7. *July 22, Michigan State University* — **Genomic sequence of grain blight.** A team of scientists has announced a genomic sequence for a grain fungus. **The genomic sequence of the fungal plant pathogen, Fusarium graminearum, has been completed, providing scientists a roadmap to combating a fungus that infects wheat and barley crops, rendering them unusable.** "We have enough to do a tremendous amount of good work," said Frances Trail, Michigan State University associate professor of plant biology. **"Now we can begin to unravel mechanisms to combat this fungus which is a devastating problem in the Midwest and all over the world."** This fungus is a serious pathogen of wheat and barley throughout the Midwest. It causes Fusarium head blight, which reduces grain yields, and taints grain with mycotoxins that have been found to be detrimental to human and animal health. **The fungus comes with a steep price tag, rendering crops worthless. For example, head blight outbreaks in the 1990s cost U.S. agriculture $3 billion.** "Classical control methods for blight just aren't working," Trail said. "Sequencing this fungus can be the beginning of designing new methods of control."
   Source: http://www.sciencedaily.com/releases/2003/07/030722073742.ht m

8. *July 22, Associated Press* — **EU says mad cow disease on the decline. The problem of mad−cow disease is diminishing in most of the 15 European Union (EU) countries, the**

EU's head office said Tuesday. In a report to EU agriculture ministers, the European Commission said its results were based on some 4.1 million tests carried out on cattle in the first five months of 2003. The tests represented about 10 percent of all cattle in the bloc. **The commission reported 591 positive cases of bovine spongiform encephalopathy from January to May, down from 603 over the same period last year.** ``The prevalance of BSE is falling in most of the member states,'' it said. In all of last year, 2,126 cases of mad−cow disease were confirmed out of 10.4 million tests mandated as part of stepped−up certification of animals meant for human consumption.
Source: http://www.guardian.co.uk/worldlatest/story/0,1280,−2937052, 00.html

9. *July 22, York Dispatch* — **More plum pox found. The Pennsylvania Department of Agriculture has identified three more peach trees infected with plum pox virus, but each was within the previously established quarantine zone and none was in an orchard.** Two infected trees were found in Adams County and a third was in York County. By the time Monday's announcement had been made, the homeowners had already removed and destroyed the trees. **So far this year, five new plum pox infections have been identified, but only one was in a commercial orchard and all have been within established quarantine zones.**
Source: http://www.yorkdispatch.com/Stories/0,1413,138~10023~1526517 ,00.html

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

10. *July 22, Water Tech Onlince* — **Water security grant awarded to rural water association.** As part of the U.S. Environmental Protection Agency's (EPA) continuing efforts to help small drinking water utilities assess their vulnerabilities to terrorist attack, EPA Assistant Administrator for Water G. Tracy Mehan has announced the award of nearly $2 million to the National Rural Water Association (NRWA). **Through this grant award, the NRWA will assist small community water systems serving populations between 3,300 and 10,000 people with security planning.** Through a combination of training sessions, on−site technical assistance, and internet based tools, the NRWA will educate system personnel about the regulation, and provide assistance in preparing vulnerability assessments and emergency response plans. **Under this project, NRWA will assist approximately 4,400 community water systems.**
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=41836

11. *July 22, Atlanta Journal Constitution* — **Governors close to deal on water use. The governors of Georgia, Alabama, and Florida said Monday they are close to settling their states' 13−year−old water conflict.** The governors extended to Aug. 31 a deadline for devising a way to share waters of the Apalachicola−Chattahoochee−Flint river system. Since negotiations over the water disputes began in February 1998, the states have extended

numerous deadlines to keep the talks alive. **At stake is enough water to quench the thirst of metro Atlanta and North Georgia residents until 2030, when the region's population is projected to reach 6 million. The governors said they have an agreement "in principle" for sharing the rivers' waters, but they do not agree on all points.** Differences include how much Lake Lanier's water levels would be drawn down during dry spells and how much water would be guaranteed to flow past the Florida state line during droughts. The states also have to work out how commercial navigation would be maintained when water levels are low. Georgia and Alabama have reached a tentative agreement on the other front in the water war, the Alabama−Coosa−Tallapoosa river system.
Source: http://www.ajc.com/metro/content/metro/0703/22waterwars.html

[Return to top]

Public Health Sector

12. *July 22, National Post* — **Transplant patients linked to SARS spread. Their immune systems weakened by anti−rejection drugs, people who have had organ transplants seem at particular risk from Severe Acute Respiratory Syndrome (SARS) and are more likely to become virus "super−spreaders," reveals a new study by Canadian scientists.** Two such patients in Toronto, including a lung recipient who was still recovering in hospital, contracted the disease and died after infecting numerous others, said one of the study's authors. At least one of those infected by the recipients also died. **In response, hospitals have developed a new screening system they hope will prevent transplant patients from getting the virus from an infected organ if there is another outbreak of SARS.** "If they are infected, they seem to have more severe disease, harder to control disease," said Dr. Deepali Kumar, lead author of the paper. **Even with the screening system in place, SARS could have a significant impact on the transplant world, which already suffers from a shortage of suitable organs, experts say. Restrictions on transferring patients between hospitals in the Toronto area meant losing 10 available donors who would have provided up to 30 donor organs, said Dr. Cameron Guest, head of the Trillium Gift of Life Network.** Having to screen out potentially infected donors in future would again curb the supply of organs, he said.
Source: http://www.nationalpost.com/national/story.html?id=901E85EB−B747−43F4−9166−F0A9AB016F03

13. *July 22, United Press International* — **CJD screening may miss thousands of cases. The U.S. government's monitoring system for cases of Creutzfeldt−Jakob disease (CJD), a fatal human brain illness, could be missing thousands of victims, scientists have said. CJD can be caused by eating beef contaminated with mad cow disease, but the critics assert without a better tracking system it might be impossible to determine whether any CJD cases are due to mad cow.** No case of mad cow has ever been detected in U.S. cattle and the Centers for Disease Control and Prevention's (CDC) monitoring system has never detected a case of CJD due to eating contaminated American beef. Nevertheless, critics say, the CDC's system misses many cases of the disease. Spontaneously−occurring CJD is a rare disorder. But several studies have suggested the disorder might be more common than thought and as many as tens of thousands of cases might be going unrecognized. **"Now people are beginning to realize that because something looks like sporadic CJD they can't necessarily conclude that it's not linked to (mad cow disease)," said Laura Manuelidis, section chief of surgery**

in the neuropathology department at Yale University. Several studies, have found that autopsies reveal 3 percent to 13 percent of patients diagnosed with Alzheimer's or dementia actually suffered from CJD.
Source: http://www.upi.com/view.cfm?StoryID=20030721−102924−4786r

14. *July 21, United Press International* — **FDA mulls blood risk of Canadian mad cow case. A recent report of a Canadian case of mad cow disease has prompted the Food and Drug Administration (FDA) to ask U.S. blood banks to assess how many donors they would lose if the agency banned people who had spent a substantial amount of time in Canada from donating blood.** The concern is variant Creutzfeldt−Jakob disease, a fatal brain illness humans can acquire from eating beef infected with mad cow disease, could be unwittingly transmitted via blood transfusions. The potential for this to occur in the U.S. was raised in May when Canadian authorities reported a cow in the province of Alberta had tested positive for mad cow disease. Dr. Jay Epstein, director of the FDA's office of blood research and review, speaking at a meeting of the agency's transmissible spongiform encephalopathies advisory committee, said the agency had requested blood banks conduct residential travel surveys to estimate the number of donors that would be lost if restrictions were imposed on people who had lived or spent time in Canada. **One concern is a Canadian ban could drastically limit the number of people who could donate, as a substantial number of people, particularly in the northern and mid−western states, have spent a substantial amount of time in Canada.**
Source: http://magazines.ivillage.com/goodhousekeeping/hb/news/article/0,,comtex_2003_07_21_up_0000−4845−bc−us−madcow−cjd−blood~ ew~xml,00.html

[Return to top]

Government Sector

15. *July 22, Government Computer News* — **New NIST spec brings contactless smart cards into the fold.** The National Institute of Standards and Technology (NIST) wants agencies to be able to use the same cards for several purposes but different smart cards for the same purpose. **To that end, it has released the Government Smart Card Interoperability Specification Version 2.1, replacing the year−old Version 2.0. The latest specification should make it easier for agencies to use smart−card systems developed by different vendors, NIST officials said.** To address a growing trend among agencies, the new standard includes a common interface for contactless smart cards, or cards that use radio frequency waves rather than physical contact to share information with a reader device. To assure interoperability, contactless cards must adhere to parts 1 through 4 of the ISO 14443 standard. Any cryptography must use algorithms approved under Federal Information Processing Standard 140−2. **The Transportation Security Administration also plans to include the new specification for its Transportation Worker Identification Card project. TSA began two TWIC pilots over the past two weeks.**
Source: http://www.gcn.com/vol1_no1/daily−updates/22844−1.html

16. *July 17, Government Executive Magazine* — **Feds urged to probe terrorist piracy rackets.** Top executives from several large anti−counterfeiting organizations and companies that own intellectual property rights on Wednesday called for the federal government to bolster efforts to stop terrorists' use of piracy and counterfeiting to fund their activities. **"Organized, violent,**

international criminal groups are getting rich from the high−gain, low−risk business of stealing America's copyrighted works," said Jack Valenti, president and CEO of the Motion Picture Association of America. "U.S. industry alone will never have the tools to penetrate these groups or to trace the nefarious paths to which those profits are put. Only governments have the tools necessary for this kind of investigation." Valenti made the comments in a written statement submitted to a House International Relations Committee hearing. He cited global examples. Timothy Trainer, president of the International AntiCounterfeiting Coalition recommended that that federal criminal statute against trafficking in counterfeit goods be strengthened and that law enforcement agencies be encouraged to cooperate on investigations. **Trainer suggested that the government study federal law enforcement agencies to assess whether investigations are trying to find potential funding links between counterfeiting and terrorist organizations.**
Source: http://www.govexec.com/dailyfed/0703/071703td2.htm

[Return to top]

Emergency Services Sector

17. *July 22, Government Computer News* — **Kentucky center tests disaster response network. The Information Technology Resource Center (iTRC) in Louisville, KY, is working with local, state and federal agencies to build a network for sharing data in the wake of a disaster such as a terrorist attack using weapons of mass destruction.** Usually six to 12 hours after a major disaster, local, state and federal officials set up a joint operations center, iTRC director Jim Graham said. **If the event involved nuclear materials, the Energy Department would send officials to the site. If biological weapons were used, the Centers for Disease Control and Prevention would send representatives. The most important element in any such scenario is communication. In the past, the communications tool of choice was radio, Graham said. But it has problems: Information can be intercepted or tapped, and often the police departments and fire departments are on different radio frequencies.** The iTRC is evaluating several applications that translate analog voice signals from radio communications into an IP data stream, using either IP or a software−defined radio. **Software−defined radio is a wireless communication, in which the transmitter modulation is generated by a computer and a receiver uses a computer to recover the signal content.**
Source: http://www.gcn.com/vol1_no1/daily−updates/22841−1.html

18. *July 16, TheOmahaChannel.com* — **Nebraska putting homeland security dollars to work. The state of Nebraska has received $32 million in federal funds since the terrorist attack of September 11. The state has, so far, spent $10 million on fighting bioterrorism and $22 million on homeland security projects.** "You constantly need to get prepared," said Lt. Gov. Dave Heineman who leads Nebraska's homeland security effort. **One of the latest projects is a video teleconferencing system for law enforcement to improve communication in emergencies. It links the state's police face to face.** "We've seen a level of integration between state agencies that we've never seen before," said Al Berndt with Nebraska Emergency Management. The state has also built a new health alert network, which Lt. Gov. Heineman said "Allows us to contact every health district in the state on a moment's notice."
Source: http://www.theomahachannel.com/news/2336489/detail.html?subi d=22100461

[Return to top]

Information and Telecommunications Sector

19. *July 22, Associated Press* — **Risks of public Internet terminals demonstrated.** The risks and dangers of using public Internet terminals at cybercafes, libraries, airports and other establishments have been demonstrated by recent high−profile cases where software that logs individual keystrokes has been installed on public computers and used to record user names and password. Neel Mehta of Internet Security Systems Inc. said that while millions of individuals use public terminals without trouble, they should be cautious. "When you sit down at an Internet cafe, ask the owner or operator about the security measures in place," he said. **Encrypting e−mail and Web sessions does nothing to combat keystroke loggers, which capture data before the scrambling occurs. Data cookies, files that help Web sites remember who you are, also contribute to the risk of identity theft. Unless you remember to log out, these files could let the next person using the public terminal to surf the Web as you.** Browsers typically record recent Web sites visited so users won't have to retype addresses. But such addresses often have usernames and other sensitive information embedded. Secure public terminals should by default have provisions for automatically flushing cookies and Web addresses when a customer leaves, Internet security experts say.
    Source: http://www.washingtonpost.com/wp−dyn/articles/A29083−2003Jul 22.html

20. *July 22, Medill News Service* — **Changes in broadband laws stall. Lawmakers are asking the Federal Communications Commission (FCC) to issue a pending Triennial Review Order that will dictate whether broadband Internet is classified as an information service or a telecommunications service, which in turn determines how it can be regulated**. Some cable operators are classified as information service providers and not as telecommunication services, they don't have to let the public or competitors use their pipelines. However, common telecommunication carriers−−notably telephone companies that also sell DSL services−−must share access. Lawmakers and panelists at a hearing of the House Energy and Commerce subcommittee Monday agreed **there are two ways to give cable and DSL services an even playing field: place broadband cable services under the same regulations currently imposed on DSL providers; or deregulate DSL companies and let them compete freely in the marketplace**. Regulating cable service providers, opponents say, would inhibit industry growth, competition, and capital investment. On the other hand, DSL providers entering a totally deregulated market could get crushed by their cable modem competitors, who control the vast majority of the market share as well as the infrastructure.
    Source: http://www.pcworld.com/news/article/0,aid,111692,00.asp

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 445 (microsoft−ds), 80 (www), 1434 (ms−sql−m), 4662 (eDonkey2000), 54846 (−−−), 113 (ident), 16058 (−−−), 139 (netbios−ssn), 12072 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

21. *July 22, FOXNews.com* — **Eiffel Tower fire extinguished. A fire broke out on the top of the Eiffel Tower on Tuesday, sending black smoke pouring from the 1,069−foot Paris landmark and forcing the evacuation of a stream of visitors. The fire −− which broke out in an area housing television and radio equipment, just below the tower's antenna −− was put out after about an hour, police said. The cause of the fire was not immediately known,** the company that operates the tower said. Officials said they were not sure whether anyone was in the area where the fire erupted. There were no immediate reports of injuries.
Source: http://www.foxnews.com/story/0,2933,92626,00.html

22. *July 22, FOXNews.com* — **Wildfires rage across central Montana. Rising temperatures and wind Tuesday threatened to revive a cluster of range fires that had burned 105,000 acres of north−central Montana, threatening isolated farm and ranch homes.** About 50 people had been evacuated as the fire blackened stands of ponderosa pine and charred pastures and hayfields. "We expect more wind today," said information officer Pat McKelvey at the main fire camp outside Jordan. The fires made little progress Monday, when the high was only in the 80s, but temperatures were headed into the 90s Tuesday, McKelvey said. Elsewhere in the West, officials in California's San Luis Obispo County discovered that three houses and several outbuildings had been destroyed by a blaze that forced some 250 people to flee an area of rolling, oak−studded hills. **Large fires also were active Tuesday in Arizona, Colorado, Idaho, New Mexico, Nevada, Oklahoma, Oregon, South Dakota, Utah and Washington, the National Interagency Fire Center said.**
Source: http://www.foxnews.com/story/0,2933,92580,00.htm

23. *July 22, The Christian Science Monitor* — **U.S. military confirms Uday and Qusay Hussein killed Tuesday. The U.S. military said Tuesday it had confirmed that Saddam Hussein's two sons, Qusay and Uday, had been killed in a fierce gun battle** in the northern city of

Mosul. U.S. troops raided a villa in the city after receiving a "walk−in" tip that the two sons were holed up there, said Lt. General Ricardo Sanchez at a news conference in Baghdad. Given the notoriety among both Iraqis and Americans of the two sons, **their deaths are seen as an important morale boost both to U.S. troops and to Iraqis beginning to doubt that the old regime was gone for good**. Despite being the younger of Hussein's two sons, **Qusay was said to be first in line to succeed his father**. He oversaw Iraq's intelligence and security services, including the notorious Special Republican Guard, and in 2001 was named deputy of the Baath Party's military bureau. **Uday was instrumental in putting down threats to his father's regime. He used blackmail, torture, imprisonment, and even murder to eliminate real or perceived enemies**. He ordered the killing of thousands of inmates throughout the 1990s, and put the lid on a Shiite revolt in 1997.
Source: http://csmonitor.com/2003/0723/p01s01−woiq.html

24. *July 22, U.S. Department of Homeland Security* — **Information Bulletin: Potential Terrorist Use of Official Identification, Uniforms, or Vehicles.** Department of Homeland Security (DHS) Information Bulletins are informational in nature and are designed to provide updates on the training, tactics, or strategies of terrorists. **The following information is meant to advise the owners and operators of the nation's infrastructures about the possible use by terrorists of official identification, uniforms, or vehicles to gain access to sensitive facilities for purposes of planning or carrying out attacks.** While DHS possesses no information indicating an organized effort by extremist elements in the United States to illegally obtain official identification, uniforms, or vehicles in furtherance of terrorist activities, it has identified the recent theft or disappearance of large numbers of these items. Attempts to acquire official identification, uniforms, or vehicles would be consistent with the tactics and techniques of Al−Qaeda and other extremist groups, according to a variety of reporting sources. In an effort to understand the extent of such thefts, DHS recently conducted a survey of selected members of the law enforcement community in five states. This survey revealed that from February to May 2003 hundreds of official identification cards, badges, decals, uniforms, and government license plates were reported stolen or lost. **DHS reminds all recipients to remain vigilant to the disappearance of, or unauthorized inquiries regarding, official identification cards, badges, decals, uniforms, government license plates, and vehicles and establish practices that account for missing items. DHS encourages recipients to report suspicious incidents to the proper authorities and to remain vigilant for any nexus to terrorism.** For more information about protective measures owners and operators can take, please see the full−text of this information bulletin.
Source: http://www.nipc.gov/publications/infobulletins/2003/Potential%20Terrorist%20Use.htm

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer